CLAIMS

What is claimed is:

1. A method of booting a computer, comprising:

testing for an intrusion into a first component; and,

configuring said first component from a stored profile if an intrusion was not detected.

2. The method of claim 1, further comprising:

constructing a profile for said first component if an intrusion was detected; and,

storing said profile for said first component.

3. The method of claim 1, further comprising:

configuring a second component from information discovered about said component.

4. The method of claim 3 wherein said information is discovered regardless of detection of an intrusion into said second component.

5. A method of booting a computer, comprising:

storing a profile for each of a plurality of components;

detecting an intrusion into at least one of said plurality of components;

discovering characteristics about said at least one of said plurality of components.

6. The method of claim 5, further comprising:

storing a new profile for said at least one of said plurality of components.

7. The method of claim 5, further comprising:

configuring a set of said plurality of components using said profile for said plurality of components wherein said set of said plurality of components are not members of said at least one of said plurality of components.

8. The method of claim 5 wherein each of said plurality of components are configured using said profile corresponding to each of said plurality of components if said intrusion was not detected into said component.

9. A computer system, comprising:

a chassis intrusion detection system; and,

a state machine that configures a component of said computer system from a stored profile of said component if said chassis intrusion detection system indicates that said component has not been altered and configures said component from information discovered about said component if said chassis intrusion detection system indicates that said component may have been altered.

10. The computer system of claim 9 wherein said chassis intrusion detection system comprises a service processor.

11. The computer system of claim 10 wherein said chassis intrusion detection system comprises switches coupled to said service processor whereby the state of at least one of said switches indicate when at least one access panel on a chassis of said computer system is open.

12. The computer system of claim 10 further comprising:

a main power supply; and,

a standby power supply that powers said chassis intrusion detection system.

13. The computer system of claim 12 wherein when said main power supply and said standby power supply are both turned off said state machine configures said component from said discovered information.

14. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for booting a computer, said method steps comprising:

reading an indicia that indicates whether a change may have been made to a component;

discovering information about said component if said indicia indicates a change may have been made to said component and configuring said component based upon said discovered information; and,

configuring said component based upon stored information if said indicia indicates a change has not been made to said component.

15. The program storage medium of claim 14 wherein said indicia corresponds to whether an access panel has been opened and to whether main and standby power have been turned off.

16. The program storage medium of claim 15 wherein a service processor that operates on standby power generates said indicia.

17. The program storage medium of claim 15 wherein a main processor communicates with said service processor to read said indicia.